PRODUCTS AND SERVICES
- Course Offerings
- Prices
- Locations and Travel Information
- Courses FAQ
- Registration
- Contact Information
- Credentials Program

Fundamentals of Incident Handling

Dates

2005 Dates

March 7-11, 2005 (SEI Pittsburgh, PA)
July 18-22, 2005 (Arlington, VA)
October 31-November 4, 2005 (SEI Pittsburgh, PA)

This course may also be offered by arrangement at customer sites. E-mail training-info@cert.org or call +1 412-268-9564 for details.

Prices (USD)

U.S.
Industry: $2625
Government: $2100
Academic: $2100

International
$5250

2005

Course Registration
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
Phone: 412 / 268-7388
FAX: 412 / 268-7401
E-mail: courseregistration@sei.cmu.edu

Course Description

This five-day course is for computer security incident response team (CSIRT) technical personnel with little or no incident handling experience. It provides a basic introduction to the main incident handling tasks and critical thinking skills that will help an incident handler perform their job. This course is recommended to those new to incident handling work.

This course is designed to provide insight into the type and nature of work that an incident handler may perform. It will provide an overview of the incident handling arena, including CSIRT services, intruder threats, and the nature of incident response activities.

Course attendees will learn how to gather the information required to handle an incident; realize the importance of having and following pre-defined CSIRT policies and procedures; understand the technical issues relating to commonly reported attack types; perform analysis and response tasks for various sample incidents; apply critical thinking skills in responding to incidents, and identify potential problems to avoid while taking part in CSIRT work. The course incorporates interactive instruction, practical exercises, and role playing. Attendees have the opportunity to participate in CSIRT hotline call scenarios and to respond to sample incidents that they might face on a day-to-day basis.

After completing this course, participants are encouraged to attend the companion course, Advanced Incident Handling for Technical Staff.

This course is part of the curriculum for the CERT-Certified Incident Handler program.

Note: There is significant content overlap between the Fundamentals of Incident Handling course and the Managing CSIRTs course. We recommend that attendees register for one course or the other, but not both.

Audience · Prerequisites · Objectives · Logistics

AUDIENCE

- new CSIRT technical staff (one to three months of experience)
- experienced CSIRT staff who would like to benchmark their CSIRT processes and skill sets against best practices
- anyone who would like to learn about basic incident handling functions and activities

PREREQUISITES

Before registering for this course, participants must

- be familiar with Internet services and protocols
- have some experience with system administration for Windows or UNIX systems

TOPICS

- understanding the CSIRT environment
- CSIRT code of conduct
- security tools for used by CSIRTs
- overview of probes, scans, and common attack types
- identifying critical information
- handling the CSIRT hotline
- triage
- overview of DNS
- analyzing incident reports
- finding contact information
- coordinating response
- PGP for CSIRTs
- handling common attacks: e-mail spoofing, bombing, and spamming; denial of service; malicious code
- working with law enforcement

OBJECTIVES

This course will help participants to

- understand the technical, communication, and coordination issues involved in providing a CSIRT service
- provide effective, reliable, and consistent CSIRT services
- learn the basics of incident handling

Course Materials

Participants will receive a course notebook and a CD containing the course materials.

LOGISTICS

Class Schedule

This five-day course meets at the following times:

Days 1-5, 9:00 a.m.-5:00 p.m.

Hotel and Travel Information
Information about traveling to SEI offices in Pittsburgh, Pennsylvania and Arlington, Virginia is available on our Travel and Lodging Web pages.

Questions about this course?
Please see our Frequently Asked Questions Web page for answers to some of the more common inquiries about SEI Education and Training. If you need more information, contact us via e-mail at training-info@cert.org or telephone at +1 412-268-9564.

Related Products and Services

Courses
Managing Computer Security Incident Response Teams (CSIRTs)
Creating a Computer Security Incident Response Team
Advanced Incident Handling
Information Security for Technical Staff

Publications
CSIRT FAQ
CERT/CC Current Activity
CERT/CC Statistics
CERT/CC Overview Incident and Vulnerability Trends
CERT/CC Tech Tips
CERT/CC Incident Notes
CERT/CC Vulnerability Notes
The CERT® Guide to System and Network Security Practices

Events
Annual Computer Security Incident Handling Conference, sponsored by FIRST.ORG, Inc.

CSIRT Development Information
CERT-Certified Incident Handler Certification
CERT Training and Education

Course Registration

2005

^ TOP

URL: http://www.sei.cmu.edu/products/courses/cert/fundamentals-incident.html
Last Modified: 13 December 2004